To: Subcommittee on Unauthorized Practice of Law and Artificial Intelligence
From: Dan Rubins and Joshua Walker
Date: February 19, 2019
Re: 1a-b. Standards and Certification Process for Legal Technology Providers

Below is a response to the AI/UPL Assignment with all of the detailed reasoning for each area. The first page is the TL;DR version more appropriate for a memo.

Unfortunately, I did not get to the insurance stuff, but generally, providers should have the higher of industry-standard for their size, or $2M/$4M G/L, & E&O. Cyber is not yet standard outside of finance and some other heavily regulated industries, but it should be required for legal tech providers given the risk. Unfortunately, I don't know what is normal there, since we don't carry that policy. I think the specific amounts would get determined later on, anyway.

Standards and Certification Process for Legal Technology Providers

Evaluate competence in two ways:

- metrics that would be accepted by an academic journal, to be confirmed by independent reviewer that has relevant scientific or academic experience

- licensed attorney working with the provider, as well as a licensed attorney as independent reviewer

Confidentiality

At a bare minimum providers should meet PCI DSS, though LCCA standards would be better. Ideally providers would meet many of the ISO27000 series standards, but this carries significant cost and would be an inappropriate barrier.

Providers need limit data leakage to 3rd parties. Alternatively, providers can build end-to-end encrypted systems and perform machine-learning on-device, or use techniques like homomorphic encryption or differential privacy.

Character Review

Just as lawyers submit to a moral character review, if a legal technology provider wants to undertake activities that would traditionally be considered the practice of law, they should be screened to protect the public from similar harms.

Availability & Disaster Recovery

Legal technology providers should have availability and infrastructure suitable for their business and their company's stage.

Review Process

Modeled on the "informal conference" of a moral character determination. List of specific areas of concern attached.

Open Questions

1. Is there authority to determine and assess a fee?

2. Should meetings be open or closed?

3. Information provided to the panel may contain trade secrets or confidential business records. Should some materials be protected from disclosure? If so, by what mechanism? How will materials be archived? Is a similar system to moral character determinations available and appropriate?

4. Should candidates be able to preempt certain people or groups (e.g. people that work for a legal automation company or a contract review company) from sitting as reviewers?

Standards and Certification Process for Legal Technology Providers

Summary

Machines, and the legal technology providers that build them, are not legally authorized to practice law under today's regulatory scheme. However, this possibility is very near and provides both potential benefits by way of enabling Access to Justice, as well as many potential harms to individuals and to society as a whole. It is the job of regulators to weigh these interests as legal technology providers look to deploy machines that arguably practice law according to current definitions.

As the modern legal profession has taken shape over the last few centuries, bar associations have helped to resolve countless ethical and regulatory issues within in the legal profession. This tradition has resulted in explicit rules of professional conduct as well as norms and customs that, at least in their highest ideal, uphold the profession's integrity and protect the public. Broadly, it is in the interest of society to retain many of these norms and customs as machines inevitably begin to automate some legal processes. To explore these issues, we evaluate the interests, uses, and harms from the perspective of the legal profession using the Model Rules of Professional Conduct. We also consider ethical issues unique to human-machine interaction, algorithmic decisions, and automating some aspects of modern legal practice.

Specifically, we seek to answer the following questions:

1. What standards should technology providers meet to have their technology licensed or excluded from UPL claims by the California State Bar? Evaluate metrics for success, ethics, competency, transparency, data security, auditability, quality control, and various insurance products like general liability, errors & omissions, cyber security/data breach.
2. What process should the State Bar follow to vet or certify technology providers?

Proposed Model

The model under discussion by the ATILS AI & UPL subcommittee would not be mandatory for legal technology companies. Rather, interested companies could voluntarily submit themselves to additional regulatory oversight by the State Bar and commit to similar ethical standards, rules, and processes as

lawyers, as well as additional insurance, transparency, and accountability requirements. In exchange, these companies could be eligible for a "safe harbor" from prosecution of Unauthorized Practice of Law (UPL) claims within the limited area they are approved to operate, following a review by technical and legal professionals. Similarly, the Bar could exempt its members that use approved technology products in their practice from similar claims of Unauthorized Practice of Law and concerns of Inappropriate Supervision. No changes would be required to civil and criminal fraud, false advertising, etc. statutes, and would continue to apply to tech companies and lawyers alike. Rather, the State Bar could decline to prosecute these companies for UPL, so long as they are in good standing and have met *all* of the ethical, competence, insurance, transparency, and review requirements proposed here.

Antitrust Concerns

While an extensive legal review of Antitrust issues would necessarily occur if the proposal moves forward, the most recent Antitrust Determination, 2018-003[1] by the State Bar Office of General Counsel provides a useful summary of some dimensions of Antitrust with respect to the State Bar. "An action may raise antitrust concerns when, for example, that action raises prices, reduces output, diminishes quality, limited choices, or creates, maintains, or enhances market power." Briefly, regarding each of these dimensions:

- Basic economic theory would predict that expanding the practice of law would increase both choice and output (a goal of this task force) and would therefore lower prices.
- The market power of entrenched participants in legal services would likely be reduced by providing more choice and competition.
- Diminishing quality is a very real and valid concern as new technologies are unproven and only infrequently exceed human performance on many tasks. It will therefore be important for the State Bar to ensure any new market participants meet or exceed human performance, perhaps even by lawyers, on relevant metrics.

Evaluating Competence with Statistics (1.1, 1.3)

While AI systems are increasingly beating human benchmarks in limited domains, their general use is still quite limited. Naturally, a primary concern for many lawyers and members of the public is how competent legal advice could even be provided by a machine. However, with sufficient limitations on scope and by limiting externalities, expert systems have arguably provided legal advice for decades through widely used tax filing systems, systems that select and draft legal forms, as well as trademark filing, and many other situations. The companies making many of these products frequently employ many lawyers as experts to inform the creation of the systems.

As machine learning systems have gained popularity in recent years, however, systems are able to learn about increasingly complex situations from previous examples, rather than simply executing an expert's distilled knowledge where they feel the options are sufficiently limited and appropriate for automation. Accordingly, performance metrics of self-learning systems are of critical importance to questions of competence, especially in relation to human benchmarks.

Machine learning evaluation metrics exist for every conceivable problem that researchers dream up and are applied with varying success. For example, the F_1 score, which combines precision and accuracy, is

[1] State Bar of California, (2018), http://www.calbar.ca.gov/Portals/0/documents/antitrust/Antitrust_Determination_2018-0003.pdf (last visited Feb 8, 2019).

frequently used to evaluate many machine learning and Natural Language Processing (NLP) systems. However, it is a simple metric, arguably too simple for many advanced NLP problems. Other common NLP evaluation metrics, like the Bi-Lingual Evaluation Understudy (BLEU) score are so imperfect they have led to no fewer than 10 new variants in as many years. While the Recall-Oriented Understudy for Gisting Evaluation (ROUGE) metric, commonly used for automatic summarization and translation tasks, provides another 6 variants for some of the same tasks. There is no consensus on which metric to use for any given machine learning task, so no one metric can or should be prescribed. Rather, a sufficient number of scientifically relevant and accepted metrics are needed to evaluate performance.

Recommendation

Legal technology providers should produce whatever scientifically valid metrics for the task that would be accepted by a peer-reviewed academic journal. When possible, metrics should be evaluated against relevant human benchmarks.

Evaluating Competence with a Professional (1.1, 1.3, 5.1-5.3)

As statistics can miss many fine details, professional evaluation and oversight of legal technology systems should be required at two different levels. First, internal oversight by a licensed attorney employed by the provider (or an advisor for early stage companies), should be required, just as junior lawyers are supervised. Second, the review board should include at least one licensed attorney with experience in the same area as the technology under review.

Confidentiality and Information Security (1.6-1.8)

Confidentiality demanded of lawyers by Rule 1.6 would be even more relevant for legal technology companies under the proposed model. The concentration of sensitive data in law firms has already proven an attractive target for malign actors with high profile attacks against large law firms that have dedicated security personnel like *Appleby*[2], *Cravath, Swaine & Moore*[3], *DLA Piper*[4], and *Weil, Gotshal & Manges*.[5] Legal technology providers are already gathering huge amounts of some of the most sensitive data from businesses and individuals, much with potentially grave consequences should these companies be breached. Yet, legal technology companies today seem no better prepared than law firms. In a survey of 503 legal technology companies in 2017, we found failing grades on the most basic web security features across 87.5% of legal tech companies, according to the widely used Mozilla

[2] The lawyers at the heart of the leak, November 5, 2017, https://www.bbc.com/news/business-41878881 (last visited Feb 8, 2019).

[3] Matthew Goldstein, *Cravath Law Firm Discloses a Data Attack*, The New York Times, December 21, 2017, https://www.nytimes.com/2016/03/31/business/dealbook/cravath-law-firm-discloses-a-data-attack.html (last visited Feb 8, 2019).

[4] Adam Janofsky, *DLA Piper CIO on 'Petya' Attack: 'The Future of the Entire Business Was At Stake,'* Wall Street Journal, December 18, 2017, https://www.wsj.com/articles/dla-piper-cio-on-petya-attack-the-future-of-the-entire-business-was-at-stake-1513635888 (last visited Feb 8, 2019).

[5] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, Wall Street Journal, March 30, 2016, https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504 (last visited Feb 8, 2019).

Observatory scoring methodology.[6] Along with competence, confidentiality would seem to be the most acute concern in expanding the practice of law.

PCI DSS

At the *absolute minimum*, any legal technology provider that hopes to provide something resembling a legal service should meet widely accepted Payment Card Industry Data Security Standard (PCI DSS), and its compliance should be independently audited. Broadly, PCI DSS has 12 requirements:

1. Use a firewall to scan network traffic.
2. Change default passwords and related vendor defaults.
3. Use appropriate encryption, hashing, and masking to protect sensitive data.
4. Encrypt sensitive data in transit over public networks.
5. Protect against malware, use and regularly update anti-virus software.
6. Build secure systems and patch vulnerabilities immediately.
7. Restrict access to sensitive data to authorized personnel, "need to know" basis.
8. Identify and authenticate system access; every person needs a unique ID.
9. Restrict physical access to sensitive data.
10. Track and monitor all access to sensitive data.
11. Test security systems and processes regularly.
12. Maintain an information security policy for all personnel.

Legal Cloud Computing Association

The Legal Cloud Computing Association (LCCA) has proposed standards (Appendix A) that are not widely adopted, but well thought out and tailored to this industry. LCCA standards go further than PCI DSS by including integrity, redundancy, confidentiality, disaster recovery, and many other areas of critical importance.[7] The LCCA standards indeed cover more areas, but are vague on some specifics, so they may require more detail for practical use.

ISO 27000 Series

The International Organization for Standardization (ISO) develops and publishes international standards across many industries, including information security. The ISO/IEC 27000 series of standards (Appendix B) for Information Security could form a well-researched and internationally recognized baseline. Notably, there are already standards in this series met by legal technology providers and accepted by courts for areas like redaction (27038), digital evidence (27042), and e-Discovery (27050-1 and 27050-2).

Recommendation

At a minimum, regulators should require legal tech providers to meet PCI DSS. It would be far safer for the consumers of legal services if regulators required higher standards, like those set forth by LCCA and the ISO/IEC 27000 series. However, we must recognize doing so imposes a barrier that will disproportionately impact smaller providers. Perhaps a revenue or volume threshold could be applied to

---

[6] Mozilla HTTP Observatory. Contribute to mozilla/http-observatory development by creating an account on GitHub, (2019), https://github.com/mozilla/http-observatory (last visited Feb 8, 2019).

[7] Standards | Legal Cloud Computing Association, , http://www.legalcloudcomputingassociation.org/standards/ (last visited Feb 8, 2019).

allow smaller providers to only meet PCI DSS and require more mature providers to also meet the higher standards.

As information security rapidly changes and standards are updated, the specific requirements should be promulgated in a way that enables and encourages periodic updates by regulators.

Confidentiality and Data Processors (1.4, 1.6)

Many machine learning models that form the basis for some AI systems are extremely compute-intensive and require specialized hardware (e.g. FPGAs, GPUs, and TPUs). The vast majority of this hardware is available from a limited number of companies (Amazon, Microsoft, Google, and a few others) and is usually located in public cloud infrastructure that is physically controlled by the cloud provider. Cloud providers may be located in different or multiple jurisdictions which can impact lawful data access requests, as demonstrated in Microsoft Corp. v. United States. While that case was recently mooted by the CLOUD Act, it provides an example of the complexity of moving increasing amounts of data into the physical control of third parties in other jurisdictions. Even more concerning is how the third-party doctrine applies when a person willingly uses a software product hosted on one of these cloud providers and architected in a way that the cloud provider could access client data. Frequently with machine learning APIs, the cloud provider can even use data it receives to improve its own machine learning models with no notice to or ownership by the ultimate client. Adding to the potential erosion of civil liberties, the cloud provider may not be able or willing to resist subpoenas or other data requests like National Security Letters (that come with a gag order) on behalf of their customer's customer.

While less common, it is currently feasible to train and execute machine learning algorithms on a client's device (i.e. phone, tablet, computer, or on-premise server) instead of sending sensitive client data to 3rd party cloud providers. Doing so enables privacy-by-design architectures that use techniques like end-to-end encryption to protect sensitive client data from third parties.

Recommendation

Legal technology providers that wish to provide a legal service should either:

1. Prevent 3rd party data access using end-to-end encryption
2. Obtain positive consent from clients knowledgeable of their rights, and that they are losing an important legal protection

If a legal technology provider uses a service where a cloud provider or other third party may access sensitive client data, they must clearly disclose this (i.e. not buried in terms of service).

End-to-end encryption could mitigate concerns over data leakage and conflicts of interest. If the technology provider has no knowledge or access to client data (this may include metadata as well as content), it seems safe for any number of parties to use the service without conducting a conflict check. Without send-to-end encryption, however, it would seem irresponsible not to conduct a conflict check on every single user, which would quickly become difficult at web scale.

Character Review

Just as lawyers must submit to a moral character review, if a legal technology provider wants to undertake activities that would traditionally be considered the practice of law, they should be screened to protect the public from similar harms. A couple recent examples of legal technology providers that would rightfully raise some concerns:

- The CEO of a legal technology provider in California had "a $559,330 judgment entered against him to settle a lawsuit charging him with impersonating a lawyer, forging legal documents and fraudulently swindling two clients."[8]
- The Board Chairman and largest investor in a legal technology startup was recently indicted by a federal grand jury for conspiracy and fraud relating to an alleged $11B accounting scheme involving his previous company.[9]

There may be valid concerns regarding individuals in key management or ownership positions, as well as the company's culture and historical regard for ethics and the rule of law. Should a company have a history of flouting regulators or harming the public, if they are on uneasy financial footing, or do not have the necessary technical skill to protect sensitive client data, the review panel should recommend corrective action or deny their application.

Availability & Disaster Recovery (1.9)

All legal technology providers should have availability and infrastructure suitable for their business and their company's stage. For example a startup in beta need not have a multi-cloud, geographically-redundant deployment. However, a more mature company providing a legal service to thousands or millions of individuals needs to have appropriate disaster recovery and business continuity plans with regular failover and disaster recovery drills. There are many existing auditors and consultants available to service this need at all stages of business.

The review panel should verify existence of disaster recovery plans, with certification from an independent auditor after a suitable size and business maturity.

Proposed Review Process

Interview/Demo

Pre-interview questionnaire and an in-person or video-conference interview with a handful of professionals covering expertise in relevant technology (i.e. machine learning, expert systems, blockchain, etc.) and at least one CA licensed lawyer. An existing model that may be useful is the "informal conference" preceding a moral character determination. The interview should cover areas and questions like the following:

- Describe business model and pricing
- System architecture overview
- Overview of security and privacy controls
- (after Jan 2020) Compliance with California Consumer Privacy Act
    - Is the system currently or expected to be subject to CCPA? 1) Revenue over $25M/yr; 2) over 50k consumers, households, or devices; or 3) earns more than ½ revenue from selling data
    - Describe/demo mechanism for obtaining positive consent for data processing

---

[8] CEO of Legal Startup Settles Lawsuit Charging Fraud, Forgery and Impersonating a Lawyer, LawSites (2016), https://www.lawsitesblog.com/2016/05/ceo-legal-startup-charged-fraud-forgery-impersonating-lawyer.html (last visited Feb 19, 2019).

[9] artificiallawyer, 'Things Will Continue As Normal' After Luminance's Lynch Charged With Fraud Artificial Lawyer (2018), https://www.artificiallawyer.com/2018/11/30/things-will-continue-as-normal-after-luminances-lynch-charged-with-fraud/ (last visited Feb 19, 2019).

    - Describe/demo mechanism for responding to data access requests
- Is potentially sensitive legal information accessible to anyone but the user? List all analytics providers or vendors that may receive user data (i.e. your GDPR service provider list). Pay special attention to screen-recording analytics tools like HotJar and Inspectlet that can easily compromise user data.
- What decisions are embedded in the software?
- How are the criteria for those decisions determined? For example, a machine learning system may learn over a corpus of legal documents, while the logic in an expert system may be constructed by a professional.
- If the system is reliant on external data, where does it come from? Is it appropriately licensed?
- How is data provenance maintained?
- Is data quality an issue? If so, how is it checked?
- Is there any attempt to explain how decisions, predictions, or results are reached?
- Is there a mechanism for both the user and people impacted by the software (these may be different) to access any decision criteria, source data, and any other materials needed question or challenge a decision?
- Mechanisms to identify and mitigate bias
- Excerpts and lessons learned from interviews with actual users
- Extensive interactive product demonstration for the members

Evaluation Metrics

A limited set of evaluation criteria covering several areas should be agreed upon by the examining authority. For example, the following sections cover areas of primary importance to protecting the public from harm by legal technology providers:

- Functional completeness
- Legal competence
- Accountability & transparency
- Compliance, security, & privacy
- Societal impacts

Procedures

The interview should not be a full code review, as that would be excessive and unlikely to actually accomplish the goal of protecting the public.

As with any human evaluation, there are potential conflict issues. It would be convenient to use an existing conflict policy from another State Bar board.

In choosing reviewers techniques like random reviewer assignment, pre-interview blinding, and other mechanisms to ensure fairness should be considered.

A standard fee covering the administrative cost of organizing the meeting as well as reasonable compensation to the reviewers should be levied, if authority to do so exists or can reasonably be obtained following a recommendation.

Open Questions

1. There may not be authority to determine and assess a fee. An alternative to direct oversight could be to license a small number of independent reviewers or organizations that make representations to the State Bar.
2. Should meetings be open or closed? Open meetings with publicly known and appointed members provides more accountability and transparency. Open meetings also may avoid some conflict issues since the pool of reviewers is known. However, open meetings could limit interest since they could expose detail rather kept private.
3. The public's business should be done in public. However, information provided to the panel may contain trade secrets or confidential business records. It is in the public interest to encourage full and complete cooperation, so should some materials be protected from disclosure? If so, by what mechanism? How will materials be archived? Is a similar system to moral character determinations available and appropriate?
4. In the course of review, trade secrets may be disclosed to the panel. Should candidates be able to preempt certain people or groups (e.g. people that work for a legal automation company or a contract review company) from sitting as reviewers?

Additional Ethical Principles

The public legal system is an integral part of a well-functioning society.

Legal technology must not interfere with or disrupt the administration of justice, limit the delivery of fair remedies, or contribute to societal imbalance. At times, public or private technology may augment, substitute, or even partially replace a legal process in the same way that arbitration can provide an alternative to a trial. However, as alternatives become available, they must not inhibit or create new barriers to existing parts of the public legal system.

One standard for suitable legal advice, whether delivered by human or machine.

It would be contrary to our concept of equal justice if technology should worsen the imbalance of our current legal system where those with means frequently receive better representation. AI in Law is still an emerging field, so it is easy to imagine technology providing a lower quality legal service through buggy software and poorly performing algorithms but this may reverse in the future. In fact, many e-Discovery systems that use machine learning technology provide far superior results than human review, but only for those who can afford such tools. As technology advances, it will become increasingly important to ensure sufficient access to legal technology, just as competent legal representation is required in criminal matters.

Legal technology must not undermine fundamental human rights or erode legal norms.

The UN Universal Declaration of Human Rights (UDHR) provides a framework for the rights that must be respected, along with the US and State Constitutions, and principles codified in Rules of Professional Conduct. Notably, UDHR Article 7 provides "All are equal before the law and are entitled without any discrimination to equal protection of the law." Accordingly, accessibility, internationalization, localization, security, and privacy are not optional.

Legal technology must be designed to limit malicious use.

Our human-mediated legal system has inherent limits that can protect society from certain excesses that technology may exacerbate. For example, an app that enables filing of a lawsuit at the click of a button could be deployed maliciously, similar to a Distributed Denial of Service (DDOS) attack in

computer security. Deliberate or inadvertent manipulation, domestic abuse, stalking, denial of access to a legal remedy, and many other potential modalities of misuse must be thoughtfully examined and mitigated where possible. Some malicious uses cannot be mitigated, but should be weighed by independent reviewers against the technology's benefits.

Openness, transparency, and public access are critical to a fair and just legal system.

Free and public access to the laws and regulations that govern us as well as to the courts that interpret them, resolve disputes, and serve justice is necessary. While commercial involvement brings many benefits, a balance between profit and public benefit is imperative.

Appendix A - ABA Model Rules of Professional Conduct

1. Client-Lawyer Relationship
   - 1.1. Competence
   - 1.2. Scope of Representation and Allocation of Authority Between Client and Lawyer
   - 1.3. Diligence
   - 1.4. Communications
   - 1.5. Fees
   - 1.6. Confidentiality of Information
   - 1.7. Conflict of Interest: Current Clients
   - 1.8. Conflict of Interest: Current Clients: Specific Rules
   - 1.9. Duties to Former Clients
2. Counselor
   - 2.1. Advisor
   - 2.2. (Deleted)
   - 2.3. Evaluation for Use by Third Persons
   - 2.4. Lawyer Serving as Third-Party Neutral
3. Advocate
   - 3.1. Meritorious Claims and Contentions
   - 3.2. Expediting Litigation
   - 3.3. Candor toward the Tribunal
   - 3.4. Fairness to Opposing Party and Counsel
   - 3.5. Impartiality and Decorum of the Tribunal
   - 3.6. Trial Publicity
   - 3.7. Lawyer as Witness
   - 3.8. Special Responsibilities of a Prosecutor
   - 3.9. Advocate in Nonadjudicative Proceedings
4. Transactions with Persons Other than Clients
   - 4.1. Truthfulness in Statements to Others
   - 4.2. Communication with Person Represented by Counsel
   - 4.3. Dealing with Unrepresented Person
   - 4.4. Respect for Rights of Third Persons
5. Law Firms and Associations
   - 5.1. Responsibilities of a Partner or Supervisory Lawyer
   - 5.2. Responsibilities of a Subordinate Lawyer
   - 5.3. Responsibilities Regarding Nonlawyer Assistance
   - 5.4. Professional Independence of a Lawyer
   - 5.5. Unauthorized Practice of Law; Multijurisdictional Practice of Law
   - 5.6. Restrictions on Rights to Practice
   - 5.7. Responsibilities Regarding Law-related Services
6. Public Service
   - 6.1. Voluntary Pro Bono Publico Service
   - 6.2. Accepting Appointments
   - 6.3. Membership in Legal Services Organization
   - 6.4. Law Reform Activities Affecting Client Interests
   - 6.5. Nonprofit and Court Annexed Limited Legal Services Programs
7. Information About Legal Services
   - 7.1. Communication Concerning a Lawyer's Services
   - 7.2. Communications Concerning a Lawyer's Services: Specific Rules
   - 7.3. Solicitation of Clients
   - 7.4. (Deleted)
   - 7.5. (Deleted)
   - 7.6. Political Contributions to Obtain Legal Engagements or Appointments by Judges
8. Maintaining the Integrity of the Profession
   - 8.1. Bar Admission and Disciplinary Matters
   - 8.2. Judicial and Legal Officials
   - 8.3. Reporting Professional Misconduct
   - 8.4. Misconduct
   - 8.5. Disciplinary Authority; Choice of Law

Appendix B - Legal Cloud Computing Association Standards

(SECTION I) SCOPE OF STANDARDS

Standard 1. Scope and Purpose

Legal Cloud Computing Association (LCCA) is an organization whose purpose is to facilitate adoption of cloud computing technology within the legal profession, consistent with the highest standards of professionalism and ethical and legal obligations. The organization's goal is to promote standards and guidelines for cloud computing that are responsive to the needs of the legal profession and to enable lawyers to become aware of the benefits of computing resources through the development and distribution of educational and informational resources.

(SECTION II) PHYSICAL AND ENVIRONMENTAL MEASURES

Standard 2. Location of Data

LCCA SaaS providers should disclose where data housed in their systems is being stored geographically and be able to restrict its movement so that it remains within a particular country.

Standard 3. Certifications

LCCA SaaS providers should host on reputable cloud services that have obtained one of the following certifications or met similar indicia. All of the certifications listed are used to gain confidence and place trust in a service organization's systems.

1. Type 2 SOC 2 certification - A Service Organization Controls ("SOC") 2 report evaluates an organization's information systems as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.
2. ISO 27001 certification - ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it provides a framework of how to manage information security in a company. The main philosophy of ISO 27001 is based on managing risks: find out where the risks are, and then systematically treat them.
3. ISO 27018 certification - ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of Personally Identifiable Information ("PII") which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

Standard 4. Geographic Redundancy

LCCA SaaS providers must have their data centers in multiple geographic locations in the event of a natural disaster. The impact of an outage at one data center can be minimized by automatic backup and redundantly provided by additional data centers.

(SECTION III) DATA INTEGRITY MEASURES

Standard 5. Encryption

LCCA SaaS should maintain data encryption protocols covering:

1. data stored at the data center, and
2. data transmitted to and from the data center

Strong encryption may protect data from unauthorized access, copy, modification or other attacks to the integrity and security of the data.

Standard 6. Testing

LCCA SaaS providers should disclose if and how frequently data testing and/or ethical hacking services are being performed on their offering. Some of the testing methods are listed below.

1. Vulnerability Scans - A vulnerability scan is the process of identifying and quantifying security vulnerabilities in an environment. It identifies security flaws based on a database of known flaws, tests a system for the occurrence of these flaws, and provides a report of exposures and the associated level of risk for each confirmed vulnerability.
2. Penetration Testing - Penetration testing is a simulation of an internal or external attack with the intention of gaining unauthorized access to systems and the data stored within the network.
3. Static Code Reviews - Static analysis code testing provides an understanding of security issues within program code. It is a systematic review of the software source code without executing the code. The main objective of this testing is to find errors in the early stages of the development cycle.
4. Dynamic Code Reviews - A Dynamic Code analysis relies on studying how the code behaves during execution. It monitors system memory, functional behavior, response time and overall performance of the system. The main objective of this testing is to find and fix any defects.

Standard 7. Limitations on Third-Party Access

LCCA SaaS providers should disclose their policies relating to restricting and allowing 3rd party access to confidential client data by their cloud service provider and its representations.

Standard 8. Data Retention Policy

LCCA SaaS providers should disclose their data retention policies. Additionally, the SaaS providers should take reasonable steps to ensure that when data is deleted from the cloud provider's environment, the cloud provider has measures in place to ensure the data is no longer available to any entity.

(SECTION IV) USERS AND ACCESS CONTROL

Standard 9. End User Authentication

LCCA SaaS providers should provide appropriate authentication protocols based on the needs of their customers. Examples include multi-factor authentication, strength of password requirements, certificate-based protocols, device authentication.

Standard 10. Addition or Suspension of a User

LCCA SasS providers should provide admin users the ability to add users and suspend users, as well as create certain limitations on users access to information.

Standard 11. Tracking

LCCA SaaS providers should enable the ability to generate detailed audit logs of user activities within their services and disclose the time period they keep such logs.

Standard 12. Addition or Deletion of Data

LCCA SaaS providers should enable the end user to have the ability to add and delete data.

Standard 13. Retrieving Data
LCCA SaaS providers should provide functionality to enable users to be able to retrieve data in a usable non-proprietary format, and restore data inadvertently deleted within a reasonable period of time.

(SECTION V) SERVICE AGREEMENT

Standard 14. Terms of Service
LCCA SaaS providers should present a clear and understandable Terms of Service. The Service Agreement should define the LCCA SaaS performance obligations with clear terms and definitions, demonstrate how performance is being measured and what enforcement mechanisms are in place to ensure the terms are being met.

Standard 15. Privacy Policy
LCCA SaaS providers should provide a clear and accessible Privacy Policy. The Privacy Policy should disclose how information supplied to the service is housed, protected, shared, manipulated, or disposed of. In general, all user information entered into a SaaS application should be treated as confidential, private information that cannot be used by the SaaS provider for any purposes other than support of system integrity and usability objectives. Furthermore, the SaaS provider should only be permitted to view any of your private information with users explicit consent.

Standard 16. Uptime Guarantee
LCCA SaaS providers should clearly state their uptime guarantee and the metrics upon which it is based. Uptime is the amount of time that a server has stayed up and running. The guarantee must clearly state how uptime is defined and what is the compensation if the uptime promise is not met.

Standard 17. Confidentiality
LCCA SaaS providers should include terms to abide by the duties of confidentiality in the Privacy Policy, thereby ensuring that the online data storage provider has an enforceable obligation to preserve users' confidentiality and security of user data.

Standard 18. Ownership of Data
LCCA SaaS providers should provide an explicit recognition of the user's ownership of the data. It should be clearly stated that the provider can not acquire any rights or licenses, including intellectual property rights, to the users data.

Standard 19. Demands for Data
LCCA SaaS providers must notify users of demands for their information by 3rd parties as soon as possible, unless the provider is specifically prohibited from doing so by law.

Standard 20. Data Breach
LCCA SaaS providers must notify users of a data breach. The SaaS providers policy covering time and method of notification should be clearly stated as well as the standard policies and practices for responding to data breaches.

Standard 21. Disaster Recovery
LCCA SaaS providers have an obligation to maintain an accurate, up-to-date and regularly tested process for recovery and continuity plans in the event of a natural disaster or business disruption.

Appendix C - ISO/IEC 27000-series

27000 — Information security management systems — Overview and vocabulary

27001 — Information technology - Security Techniques - Information security management systems — Requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.

27002 — Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS

27003 — Information security management system implementation guidance

27004 — Information security management — Monitoring, measurement, analysis and evaluation[10]

27005 — Information security risk management[11]

27006 — Requirements for bodies providing audit and certification of information security management systems

27007 — Guidelines for information security management systems auditing (focused on auditing the management system)

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on auditing the information security controls)

27009 — Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the ISO27K standards

27010 — Information security management for inter-sector and inter-organizational communications

27011 — Information security management guidelines for telecommunications organizations based on 27002

27013 — Guideline on the integrated implementation of 27001 and ISO/IEC 20000-1 (derived from ITIL)

27014 — Information security governance.[12] Mahncke assessed this standard in the context of Australian e-health.[13]

ISO/IEC TR 27015 — Information security management guidelines for financial services - Now withdrawn[14]

ISO/IEC TR 27016 — information security economics

27017 — Code of practice for information security controls based on 27002 for cloud services

27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC TR 27019 — Information security for process control in the energy industry

27031 — Guidelines for information and communication technology readiness for business continuity

27032 — Guideline for cybersecurity

27033-1 — Network security - Part 1: Overview and concepts

27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security

27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

27033-4 — Network security - Part 4: Securing communications between networks using security gateways

27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

27033-6 — Network security - Part 6: Securing wireless IP network access

27034-1 — Application security - Part 1: Guideline for application security

27034-2 — Application security - Part 2: Organization normative framework

27034-6 — Application security - Part 6: Case studies

27035-1 — Information security incident management - Part 1: Principles of incident management

27035-2 — Information security incident management - Part 2: Guidelines to plan and prepare for incident response

27036-1 — Information security for supplier relationships - Part 1: Overview and concepts

27036-2 — Information security for supplier relationships - Part 2: Requirements

27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

27036-4 — Information security for supplier relationships - Part 4: Guidelines for security of cloud services

27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

27038 — Specification for Digital redaction on Digital Documents

27039 — Intrusion prevention

27040 — Storage security[15]

27041 — Investigation assurance

27042 — Analyzing digital evidence

27043 — Incident investigation

27050-1 — Electronic discovery - Part 1: Overview and concepts

27050-2 — Electronic discovery - Part 2: Guidance for governance and management of electronic discovery

ISO 27799 — Information security management in health using 27002 - guides health industry organizations on how to protect personal health information using 27002.

To: Subcommittee on Unauthorized Practice of Law and Artificial Intelligence
From: Wendy Chang
Date: February 19, 2019
Re: 1c. Process for enforcement standards

This memo provides a broad outline of the current Attorney discipline system in California, for discussion at the February 28, 2019 meeting about structure of possible consequences for violation of a contemplated system for registered legal technology companies.

1. California Attorney Discipline System
    a. Pre-Charge Investigation
        i. Occurs at the Office of Chief Trial Counsel ("OCTC")
        ii. Confidential (B&P Code 6086.1(b))
        iii. Inquiry Stage
            1. Intake Unit receives information and/or complaint, does preliminary investigation and decides whether to open an investigation
            2. Attorney may be contacted to provide information
            3. Many complaints resolve at this stage
                a. Closed with no action – no merit to the complaint, complainant refusal to cooperate, or other reasons (without prejudice)
                    i. Some of these are closed without ever contacting the attorney.
                b. Referral to local bar discipline mediation program (attorney participation mandated)
                c. Closure with confidential directional letter – is not discipline; points out there is potential for future violation if specific conduct is not corrected and provides resources for attorney to consult to assist in compliance
                d. Closure with confidential warning letter – is not discipline; reflects OCTC's opinion that professional misconduct has occurred but does not warrant further prosecution. Letter warns not to continue or repeat the conduct.
                e. Reference to Enforcement Unit for formal investigation
        iv. Investigation Stage
            1. Enforcement Unit may open an inquiry on its own or on reference from the Intake Unit, after receipt of communication regarding conduct of an attorney
            2. Purpose is to determine if there is reasonable cause to believe that an attorney has violated the State Bar Act or the Rules of Professional Conduct, and if there is sufficient evidence to support that allegation. (State Bar Rule Proc. 2401).
            3. Potential Resolutions:

a. Same possibilities as Inquiry closures (a)-(e);
b. Admonition – is not discipline. Fact of admonition may be communicated to complainant but is not otherwise public.
c. Agreement in Lieu of Disciplinary proceedings. Agreements may consist of conditions of practice, further legal education or "other matters". These agreements may be used in subsequent disciplinary proceedings.
d. Stipulations for discipline – stipulations as to facts, culpability and applicable discipline without need for formal proceedings other than to approve the stipulation, and if appropriate, refer to California Supreme Court.
e. Notice of Intent to File Notice of Disciplinary Charges
    i. Invitation to meet prosecutor to attempt to resolve within 20 days
        1. Settlement discussions
    ii. Early Neutral Evaluation Conference – within 15 days of request
        1. Evaluation before a State Bar Judge
        2. Settlement discussions
f. Filing of Notice of Disciplinary Charges

b. Filing of Notice of Disciplinary Charges
    i. Charges filed by Office of Chief Trial Counsel – this is an initial pleading
        1. Reasonable cause to believe Attorney violation of State Bar Act or Rules of Professional Conduct
        2. Attorney has received fair, adequate and reasonable opportunity to deny or explain the matters that are the subject of the notice
    ii. Matter moves to State Bar Court for litigation and trial for findings and a recommendation for discipline, if prosecution is successful
        1. Hearing Department (trial level)
        2. Review Department (Appeal)
c. California Supreme Court reviews recommendations for probation, suspension or disbarment, and either approves the recommendation of the State Bar Court, or it takes other action
d. Potential discipline:
    i. Admonition – is not discipline
    ii. Private Reproval
    iii. Public Reproval
    iv. Suspension/probation
    v. Disbarment

2. Discussion points for February 28, 2019 meeting
    a. Alternative 1: Parallel System
        i. Is a parallel system desirable or is it too complicated?
        ii. If too complicated – possible options

1. Creation of a modified system of discipline within the Bar with fewer layers?
2. Issue: Current system does not discipline law firms but only discipline attorneys in the law firms
    a. Require an in-house attorney to be responsible for the compliance of the company, the same way the State Bar looks at managing attorneys for law firms?
3. Creation of a 1 strike = revocation + referral for criminal prosecution system?
    a. Issue: Elimination of progressive discipline system may result in overly harsh results, which harms consumer choice and creates commercial uncertainty for legal technology companies.

b. Alternative 2: creation of a nonprofit entity whose sole purpose is to act as the registration and disciplinary authority for registered legal technology companies
    i. Pros:
        1. Takes the responsibility away from State Bar and Office of Chief Trial Counsel
        2. Resources
        3. Does not require Legislative or California Rule changes
    ii. Cons:
        1. Lack of control of the process for the State Bar and the Office of Chief Trial Counsel
        2. Lack of commercial certainty for legal technology companies may be severely hinder (fatally?) success of the program
        3. Staffing
        4. Privilege and confidentiality issues
c. Alternative 3: do nothing more on the discipline side. UPL Violators are referred for criminal action, potential discipline for attorney aiders/abettors, and civil exposure for officers and directors.

To: Subcommittee on Unauthorized Practice of Law and Artificial Intelligence
From: Heather Morse
Date: February 15, 2019
Re: 1.d Standards of corporate responsibility and enforcement

What standards of corporate responsibility should providers of licensed technology be held to? How can this be enforced?

I conferred with our corporate department regarding the question posed. At this time, they do not see how the State Bar could hold an individual corporate officer accountable to its ethical guidelines. The power of the Bar would be to decertifying the company, or, if there is a lawyer involved, that individual could be held for discipline by the State Bar.